



Elastix SIP Firewall

Manual de Usuario

Derechos de Autor

Copyright © 2014 Elastix®. Todos los derechos reservados.

Ninguna parte de esta publicación puede ser copiada, distribuida, transferida, transcrita, almacenada en ningún sistema o traducida a ningún idioma humano o de computación sin previa autorización por escrito por parte de <http://www.elastix.org>. Este documento ha sido preparado para uso de personal profesional y debidamente capacitado, y el cliente asume la completa responsabilidad al hacer uso de él.

Derechos de Propiedad.

La información de este documento es Confidencial de Elastix® y es legalmente confidencial. La información y este documento están destinados exclusivamente a su destinatario. El uso de este documento por parte de cualquier otra persona para cualquier otro uso no está autorizado. Si usted no es el destinatario exclusivo, cualquier divulgación, copia o distribución de esta información está prohibida y es ilegal.

Descargo de Responsabilidad

La información de este documento está sujeta a cambios sin previo aviso y no debería interpretarse como un compromiso por parte de **<http://www.elastix.org>**. Y no asume ninguna responsabilidad o establece ninguna garantía contra errores que puedan aparecer en este documento. Puede aparecer en este documento y rechaza cualquier garantía implícita de comercialización o aptitud para un propósito en particular.

1.1. Sobre este manual

Este manual describe la aplicación del producto Elastix® y explica cómo trabajar y usar las características principales. Sirve como medio para describir la interfaz de usuario y cómo usarla para lograr tareas comunes. Además, este manual describe las premisas y los usuarios subyacentes que hacen la información del modelo subyacente.

1.1. Uso del Documento

En este manual, algunas palabras están representadas con diferentes fuentes, tipos de letra, tamaños y peso. La selección resaltada es sistemática; diferentes palabras están representadas en el mismo estilo para indicar su inclusión en una categoría específica. Además, este documento tiene diferentes estrategias para atraer la atención del Usuario hacia ciertas piezas de información. De acuerdo a cuán crítica es la información para su sistema, estos ítems están marcados como una nota, sugerencia, importante, precaución o advertencia.

Ícono	Propósito
	Nota
	Sugerencia/Práctica Adecuada
	Importante
	Precaución
	Advertencia

- **Negrita** indica el nombre de los ítems, opciones, cuadros de diálogos, ventanas y funciones del menú.
- El color azul con un subrayado es usado para indicar referencia cruzada e hiperenlaces.
- Párrafos Enumerados – Los Párrafos Enumerados son usados para indicar tareas que necesitan ser realizadas. El texto en los párrafos sin enumerar representa información común.
- La fuente Courier indica una secuencia de comando, tipo de archive, URL, nombre de Carpeta/Archivo Ej.: <http://www.elastix.org>

1.2. Información de Ayuda

Se han realizado todos los esfuerzos para asegurar la precisión del documento. Si usted tiene comentarios, preguntas o ideas con respecto al documento, contáctese a:

sales@elastix.com

Índice

1.1. Sobre este manual.....	2
1.1. Uso del Documento	2
1.2. Información de Ayuda	3
1. Introducción	6
1.1 . Resumen:.....	6
1.1.1. Leds de Notificación (Sobre el Panel Frontal del SIP Firewall).....	8
1.1.2. Vista Trasera del SIP Firewall:	9
1.1.3. Consideraciones de Implementación del SIP Firewall	9
2. Instalación y Configuración Inicial	11
2.1 .Configuración por Defecto	11
2.2. Acceso a la WebUI	11
2.4 Expiración de Sesión de la WebUI	14
2.5 Configuraciones WebUI	14
2.4 Panel.....	15
3. Configuración de Dispositivo	16
3.1. Configuraciones Generales	17
3.2. Configuraciones de Hora	18
3.3. Gestión de Acceso.....	19
3.4. Actualización de Firma	20
3.5. Registro	21
4. Configuración de las Políticas de Seguridad SIP	22
4.1. Políticas de Detección de Ataques SIP	22
4.2. Protocolo de Cumplimiento SIP	24
4.3. Normas Firewall.....	27
4.4. Configuración de Firewall	27
4.5. Normas de Lista Blanca.....	28
4.6. Normas de Lista Negra (Estática).....	29
4.7. Normas de Lista Negra Dinámica	30
4.8. Filtro IP Geo.....	31
5. Estado	32
5.1. Alertas de Seguridad	32

6. Herramientas	33
6.1. Administración	33
6.2. Diagnósticos	34
6.3. Ping	35
6.4. Trace Route	35
6.5. Solución de Problemas	36
6.6. Actualización de Firmware	37
6.7. Archivo de Registros	38
 APÉNDICE.....	 39
 7. Apéndice A – Usando Acceso de Consola	 39
 8. Apéndice B – Configuración de la Dirección IP del SIP Firewall a través de la Consola	 40

1. Introducción

1.1 . Resumen:

Este manual de Usuario describe los pasos que consisten en la instalación del Appliance Elastix® SIP Firewall. Elastix® SIP Firewall es un equipo basado en la solución de prevención de amenazas VoIP dedicado a proteger las implementaciones de dispositivos de Gateway/IP (Puerta de Enlace/IP), PBX/Telecom basados en SIP (Protocolo de Inicio de Sesiones). El appliance realiza la Inspección Profunda de Paquetes en el tráfico SIP para identificar los vectores de ataque VOIP y previene las amenazas que impactan en los dispositivos basados en SIP. El equipo ha sido creado para integrarse perfectamente con la infraestructura de red existente y reduce la complejidad de implementación.

El set de características del appliance incluye,

- Analizar los paquetes SIP usando el *motor de Inspección Profunda de Paquetes*.
- Detección de Anomalías de Protocolo SIP con configurabilidad de parámetros de detección.
- Detección y Prevención de las siguientes categorías de Ataques basados en SIP
 - Ataques de Reconocimiento (Huellas Digitales de Dispositivos SIP, enumeración de Usuario, Intención de Decodificar Clave)
 - Ataques de Dos/DDos
 - Ataque basados en Escritura de Sitios Cruzados
 - Ataques de búfer overflow
 - Ataques basados en Anomalías SIP
 - Vulnerabilidades de proveedores de 3ros.
 - Detección y prevención de Fraude Telefónico
 - Protección contra VOIP SPAM y War Dialing
- La respuesta al ataque incluye la opción de declinar discretamente paquetes de SIP maliciosos para ayudar a prevenir los continuos ataques
- Servicio de Actualización de Lista Negra Dinámica para Amenazas VOIP, SIP Gateway/PBX
- Configurabilidad de normas de Lista Negra/Lista Blanca/Firewall.
- Soporte para bloqueo basado en Localización Geo
- Proveer la opción de asegurar contra las vulnerabilidades de Aplicación de PBX
- Operar en dispositivos de Capa 2, por consiguiente, transparentes para la infraestructura existente IP – no se requieren cambios para agregar el dispositivo a su red existente.
- Gestión de Acceso del Dispositivo basado en Web/SSL el cual permitirá gestionar el dispositivo desde cualquier lugar desde la Nube.
- Habilidad para restringir la gestión de acceso del dispositivo para Redes/IP específicas.

- Suministrar a eventos de Estado/Seguridad del Sistema opciones de inicio de sesión para un servidor remoto Syslog.
- Suministra el rendimiento SIP hasta ~10Mbps.
- Soporte para la suscripción de actualización de Firma y mecanismos de actualización de firma.
- El dispositivo ha sido creado para operar con configuración por defecto con solo encender el dispositivo. No se requiere intervención del administrador para operar el dispositivo con la configuración por defecto.
- Suministro de energía basada en USB
- Soporte opcional para registro de eventos de seguridad en el almacenamiento basado en USB.

Especificaciones Técnicas

Modo Funcional	Firewall Transparente con Motor de Paquete Profundo SIP.
Intrusión/Prevención de SIP	Soporte de Firmas de Ataques SIP ~400+
Rendimiento	~10Mbps
Nro. de llamadas simultáneas que soporta	Hasta 50 llamadas simultáneas
Registro	Consola de Eventos de Seguridad Local, Syslog Remoto
Gestión de Dispositivo	Web GUI a través de Https y SSH CLI
Hardware	Procesador de Núcleo Individual de 32bit, basado en MIPS, 300MHz
Almacenamiento Primario	16 MB Flash
RAM	64MB
Almacenamiento Secundario	Soporte de dispositivos de Almacenamiento USB para registro (Opcional)
Interfaces	Dos Interfaces de Ethernet Rápidas.

1.1.1. Leds de Notificación (Sobre el Panel Frontal del SIP Firewall)

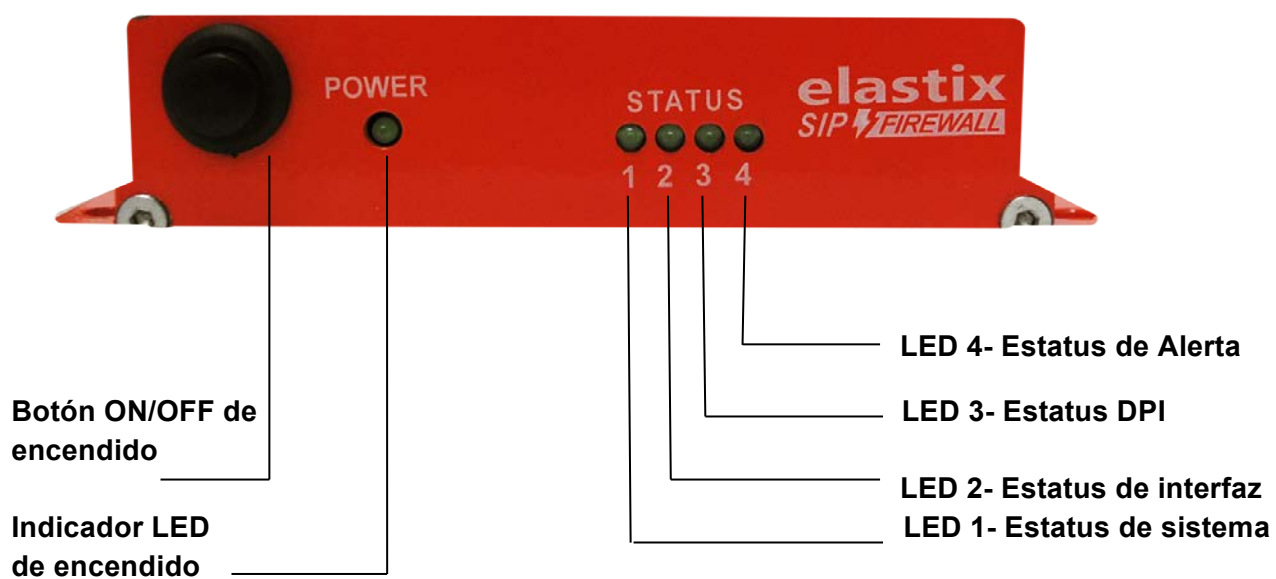


Figura 1: Notificaciones Led del Panel Frontal

El paquete SIP Firewall incluye:

- 1 Appliance SIP Firewall
- 1 Adaptador de Corriente USB
- 1 Cable de Consola Serie
- 2 Cables Ethernet

1.1.2. Vista Trasera del SIP Firewall:

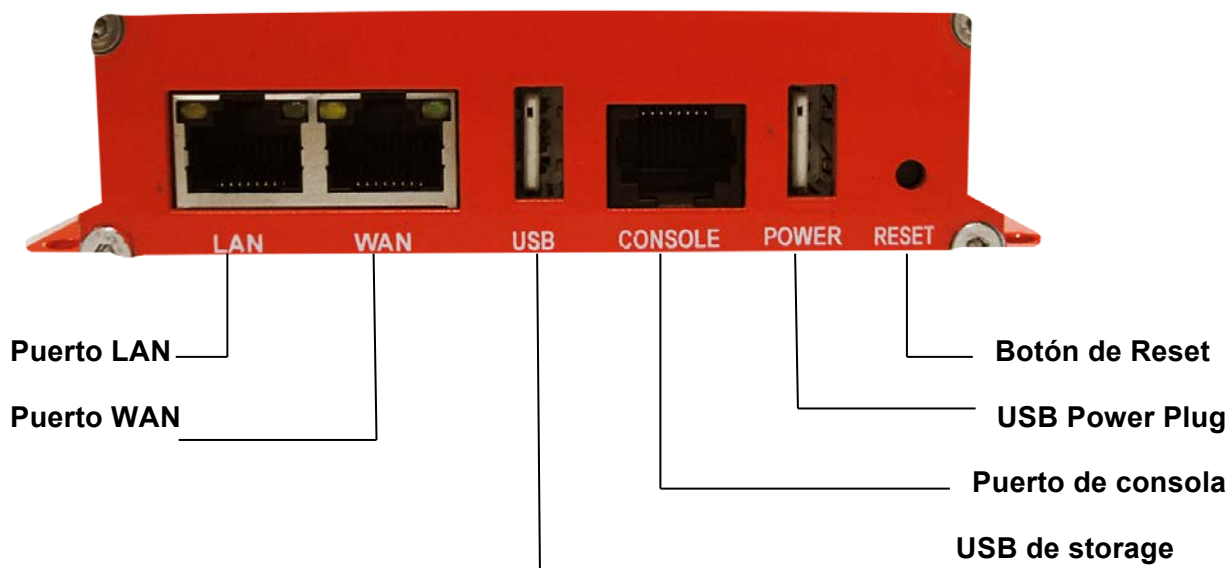


Figure 2: Vista Trasera del SIP Firewall

1.1.3. Consideraciones de Implementación del SIP Firewall

El SIP Firewall ha sido creado para proteger a los Servidores Gateway/PBX basados en SIP contra las amenazas y anomalías de red basadas en SIP. Por consiguiente, se recomienda implementar el SIP Firewall junto con la implementación del Gateway/PBX como se indica en los siguientes supuestos basados en lo que es aplicable en la instalación del usuario.

Supuesto de Implementación 1

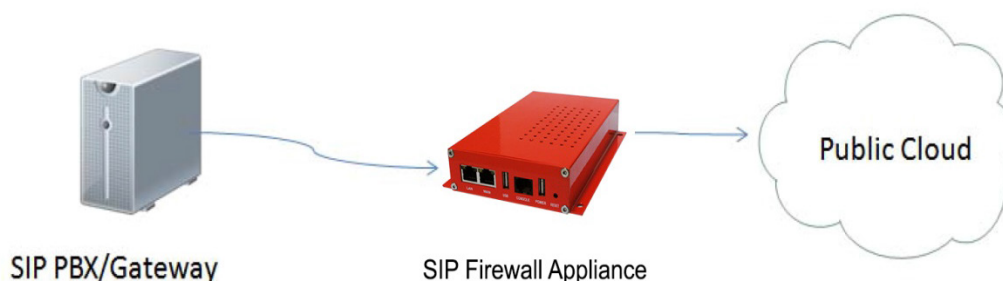


Figura 1: Supuesto 1



Algunos de los dispositivos PBX/Gateway tienen una interfaz exclusiva LAN/Mgmt para el propósito de gestión de dispositivo además de una Interfaz de Datos (además denominado Interfaz WAN/Pública). En dichos casos, el Puerto LAN del SIP Firewall debe ser conectado a la Interfaz de Datos (WAN/Interface Pública).

Supuesto de Implementación 2

En el caso del IPPBX implementado en la Instalación LAN, se recomienda la siguiente instalación, ya que ayudará a proteger contra las amenazas tanto de la Red Interna, así como también amenazas de la Nube Pública que penetraron un firewall estándar de la empresa no dedicado a SIP.

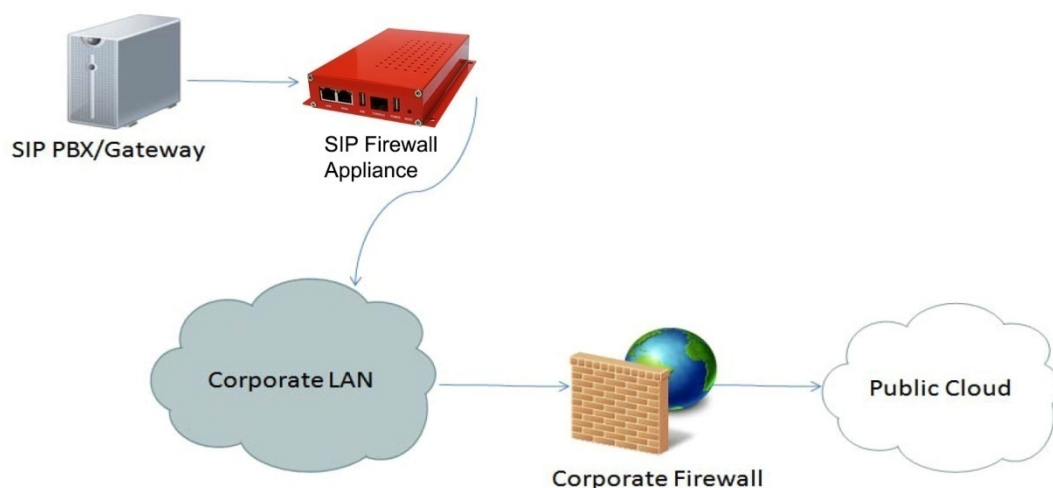


Figura 2: Supuesto 2

Supuesto de Implementación 3

En el caso de que se implementen múltiples Gateway IPPBX/ VOIP en la Instalación LAN, se recomienda la siguiente instalación, ya que ayudará a proteger contra las amenazas tanto de Red Interna como amenazas de la Nube Pública que penetraron la penetraron un firewall estándar de la empresa no dedicado a SIP.

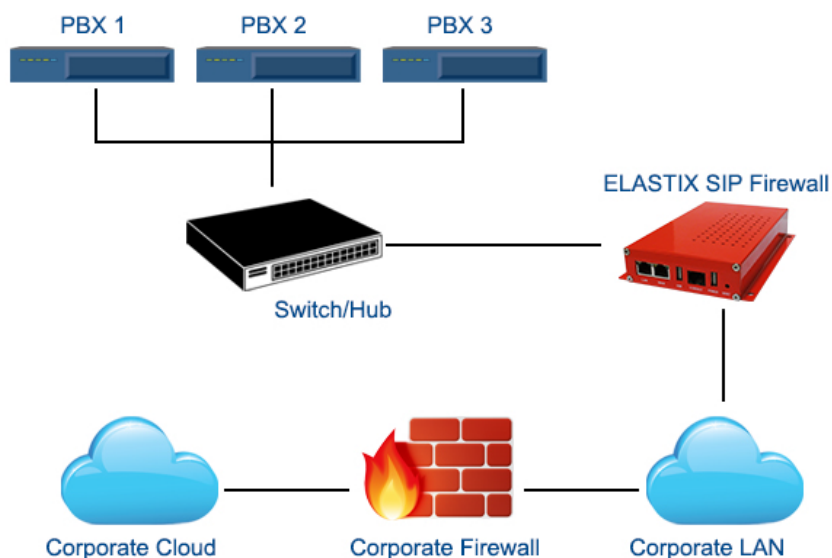


Figura 3: Supuesto 3

2. Instalación y Configuración Inicial

1. Retire los items de la caja
2. Revise que tenga todos los ítems listados en el contenido del paquete.
3. Conecte el puerto WAN del SIP Firewall a la red no confiable/pública.
4. Conecte el puerto LAN del SIP Firewall a la Gateway PBX/VOIP.
5. Conecte el equipo a la toma de corriente usando el cable de alimentación USB.
6. El dispositivo se tomará alrededor de un minuto para arrancar y funcionará completamente con la configuración por defecto.



Algunos de los dispositivos PBX/Gateway pueden tener una Interfaz exclusiva LAN/Mgmt para propósitos de gestión del dispositivo además de la Interfaz de Datos (además denominada WAN/Interfaz pública). En dichos casos, el puerto LAN del SIP Firewall debe ser conectado a la Interfaz de Datos (WAN/ Interfaz Pública).

2.1 .Configuración por Defecto

El dispositivo funciona como un puente firewall transparente con Inspección Profunda de Paquetes habilitada en el tráfico SIP. Por defecto, el equipo ha sido configurado con IP estática de 10.0.0.1 (Máscara de red 255.255.255.0)

El dispositivo ha sido creado para ser completamente funcional con la configuración por defecto. Sin embargo, si el usuario necesita mejorar las configuraciones y las políticas de DPI del dispositivo, el usuario puede mejorar la configuración a través de la WebUI del Dispositivo.

El dispositivos provee una interfaz de línea de comando accesible a través de SSH, la cual permitirá configurar los marcos básicos y visualizar el estado del dispositivo.

Gestión de Acceso	Credenciales de Registro
WebUI	admin/admin
SSH CLI	admin/stmadmin
Management Vlan IP	192.168.100.1/255.255.255.0
Default Device IP	10.0.0.1/255.255.255.0

2.2. Acceso a la WebUI

El usuario se puede conectar al dispositivo a través de la Vlan (red de área local virtual) de gestión para acceder a la WebUI (interfaz de usuario) durante la instalación inicial. La

Vlan configurada en el dispositivo, es accesible a través de puertos LAN/WAN y se fabricó con la dirección IP asignada '192.168.100.1' por defecto.

Siga el procedimiento de abajo para acceder a la WebUI,

1. Conecte el puerto LAN del SIP Firewall a la PC.
2. Asigne la dirección IP 192.168.100.2 a la PC. Establezca la máscara de Red como 255.255.255.0.

Ahora usted puede acceder al dispositivo desde el navegador usando la URL <https://<192.168.100.1>>

Configure la Dirección IP del Dispositivo SIP Firewall desde la página de "Device Settings" (Configuraciones de Dispositivos) según la configuración de su red local. Verifique la dirección IP establecida en el SIP Firewall desde la página del panel. Una vez que el usuario asigna la Dirección IP del Dispositivo SIP Firewall con éxito, ya puede acceder al dispositivo usando esa dirección IP.

Ahora puede desconectar la PC y conectar el puerto LAN a la Red PBX/PBX que necesita ser protegida.



La WebUI ha sido creada accesible solo a través de HTTPS. El navegador recomendado para acceder a la SIP Firewall WebUI es Mozilla Firefox.



La UI le permite al administrador configurar la gestión de direcciones Vlan IP. En caso de que el usuario haya cambiado la gestión de la dirección Vlan IP, necesita asignar la dirección de red correspondiente a su PC para la gestión de acceso subsecuente. Al lanzar la WebUI del SIP Firewall, la aplicación web inmediatamente solicitará las credenciales del administrador para iniciar sesión.



Alternativamente, el usuario puede acceder al dispositivo a través de la IP estática 10.0.0.1 y configurar los marcos de la red durante la primera instalación. Conecte una PC al puerto LAN del SIP Firewall y asigne la dirección IP 10.0.0.100/255.255.255.0 a la PC. Ahora usted puede acceder al dispositivo desde el navegador usando la URL <https://<10.0.0.1>>



Si el dispositivo no es accesible luego de configurar la nueva configuración de red, intente reiniciar el dispositivo y revisar el acceso al panel del dispositivo a través de la Gestión Vlan.

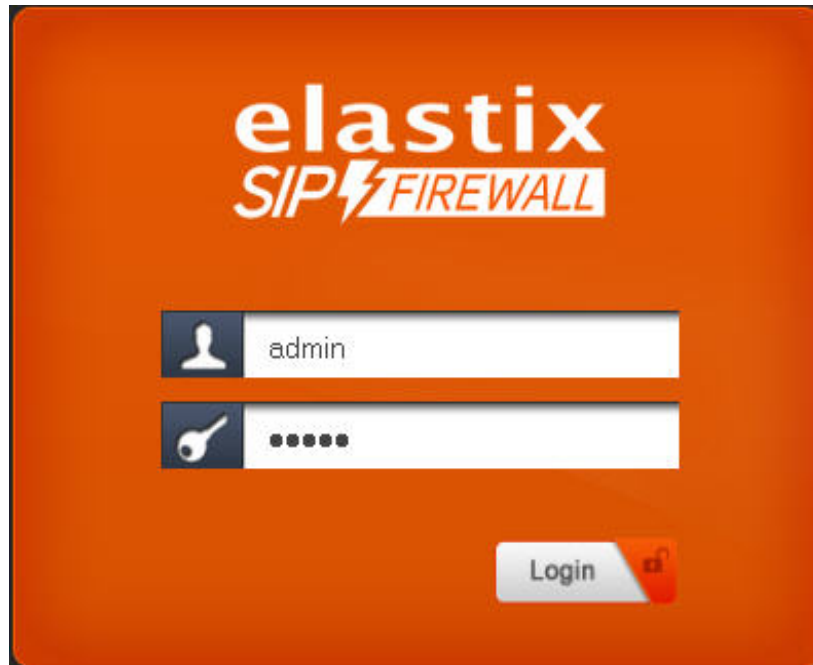


Figura 4: Página de Login

La sesión de login de la WebUI ha sido creada para expirar, y si el usuario no ingresa las credenciales de login durante los 30 segundos será redirigido a la página informativa. El usuario puede hacer clic en el hipervínculo mencionado como 'login' que aparece en la página de información para volver a visitar la página de login.

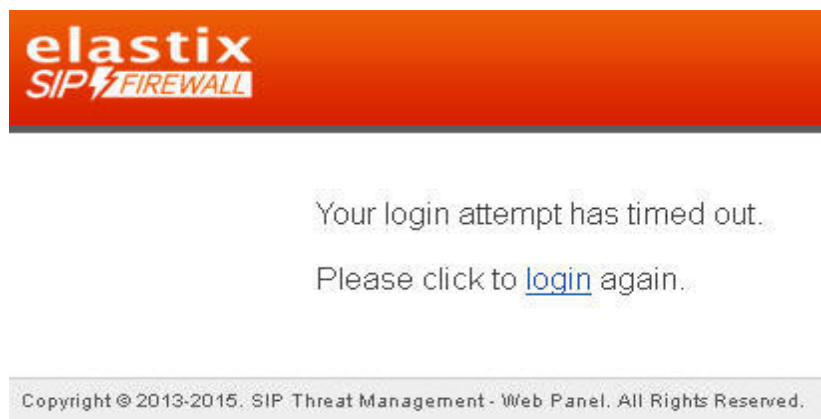


Figura 5: Mensaje de expiración

Si alguien ya inició sesión en la sesión SIP Firewall WebUI, los intentos subsecuentes para iniciar sesión notificarán los detalles de inicios de sesión previos como es ilustrado abajo y le solicitará al usuario ignorar el inicio de sesión previo y continuar O descartar el intento de inicio de sesión.

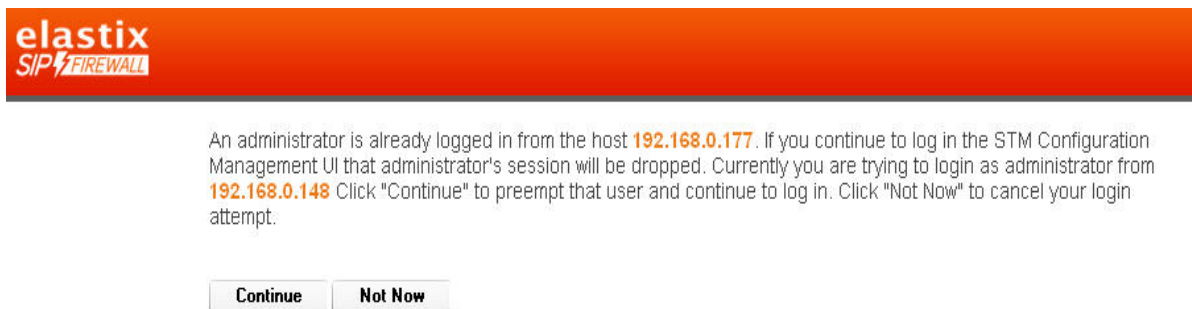


Figura 6: Seleccione Intento de login

2.4 Expiración de Sesión de la WebUI

Luego de registrarse en la WebUI, si no hay actividad hasta el período de expiración de la sesión WebUI (Por defecto, la expiración de la sesión WebUI está establecida en 900 segundos), entonces la sesión de login terminará automáticamente y el navegador será redirigido a la página de login nuevamente.

2.5 Configuraciones WebUI

Para cambiar las configuraciones de la WebUI, haga clic en el ícono de configuraciones que aparece sobre la esquina superior derecha (debajo del botón Apply Changes (Aplicar Cambios)). El diálogo de configuraciones WebUI se mostrará en el navegador y le permitirá al administrador configurar la expiración de sesión WebUI y la clave de login WebUI. Para configurar la clave de login WebUI, el usuario necesita ingresar la clave de administrador establecida previamente.

The image shows a 'Web Settings' dialog box with an orange header bar containing the title 'Web Settings' and a close button (X). The dialog contains five configuration fields, each with a label and a text input box: 'Session Timeout : 900', 'User Name : admin', 'Old Admin Password :', 'New Admin Password :', and 'Confirm Admin Password :'. Each input box has a small information icon (i) to its right. At the bottom right of the dialog are two buttons: 'SAVE' (orange) and 'CANCEL' (gray).

Figura 7: Configuraciones de la WebUI

2.4 Panel

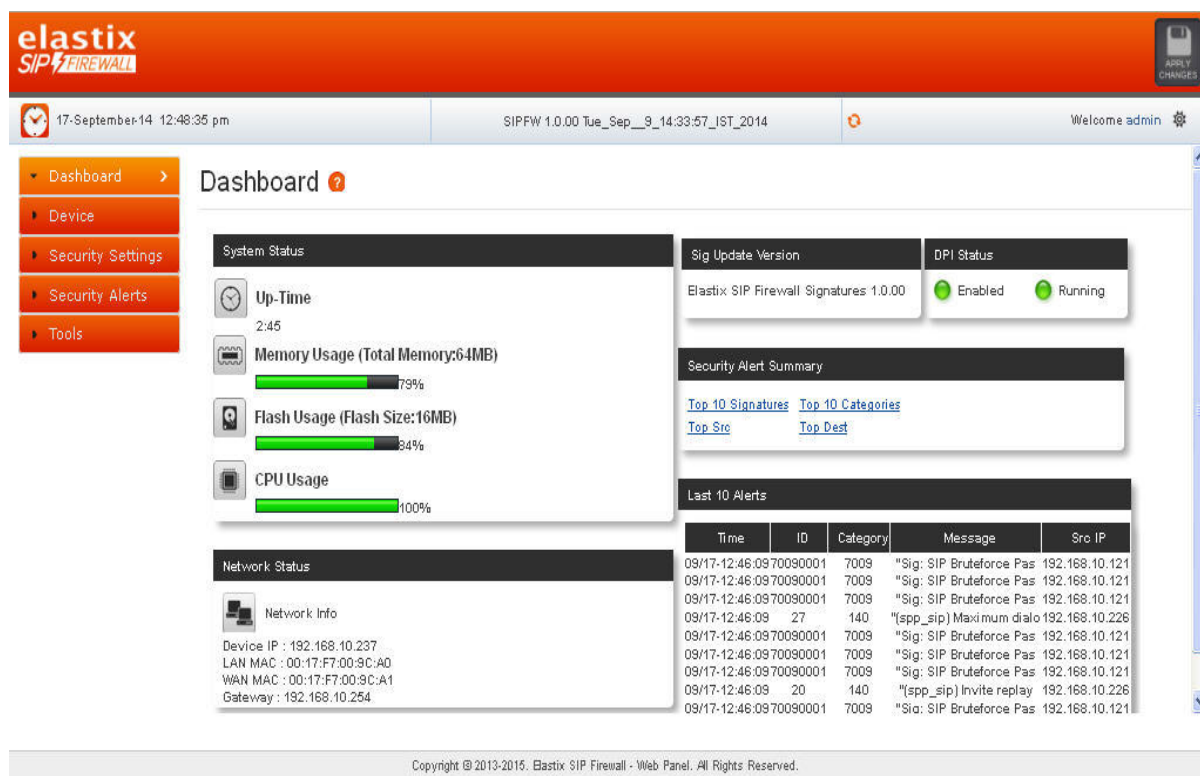


Figura 8: Panel

Al ingresar al WebUI del SIP Firewall, se mostrará el panel.

El usuario puede visitar la página del panel desde cualquier página de configuración en el WebUI del SIP Firewall, haciendo clic en el Ícono del Producto SIP Firewall que aparece en la esquina izquierda del Panel superior.

El panel de estado que aparece abajo del panel superior muestra las configuraciones de tiempo en el dispositivo y la versión de firmware del SIP Firewall, el ícono para volver a cargar la página y el ícono de Configuración.

Haciendo clic en el botón de volver a cargar la página, se volverá a cargar el área del contenido principal de la página actual.

Haciendo clic en el ícono de configuraciones, el menú emergente que contiene opciones de menú para cerrar sesión, se mostrarán las configuraciones WebUi.

El Panel de Estado del Sistema muestra el tiempo, el Uso de Memoria, el Uso de Flash y el Uso de CPU del Dispositivo. El Panel de Versión de Actualización Sig muestra la versión de Firma SIP Firewall y el Estado de Lanzamiento. El Panel de Estado de Red muestra la IP, LAN MAC, WAN MAC y Gateway del dispositivo.

El Panel de Resumen de Alerta de Seguridad muestra hiperenlaces para visualizar los hits de las 10 Firmas Principales, los hits de las 10 Categorías Principales, las Direcciones IP de los Atacantes Principales y los 10 destinos objetivo Principales.

3. Configuración de Dispositivo

Las páginas de configuración en la WebUI del SIP Firewall han sido creadas para configurarlo de forma autónoma y con facilidad.

Todas las páginas de configuración han sido creadas para trabajar bajo modelo de dos fases (grabar y aplicar cambios).



El modelo de dos fases no es aplicable a las configuraciones de tiempo y las configuraciones de actualización de firma. En estas configuraciones, los cambios serán aplicados directamente al hacer clic en 'Apply' (Aplicar) en el área de contenido del editor de configuración.

Esto es, Cuando el administrador cambia las configuraciones en las páginas de configuración y hace clic en el botón Save (Guardar), las configuraciones serán guardadas en una ubicación de almacenamiento temporaria en el dispositivo. Al guardar los cambios de la configuración, el botón 'Apply Changes' (Aplicar Cambios) que aparece en la esquina superior derecha será habilitado, y el botón 'Ignore Changes' (Ignorar Cambios) aparecerá al lado.

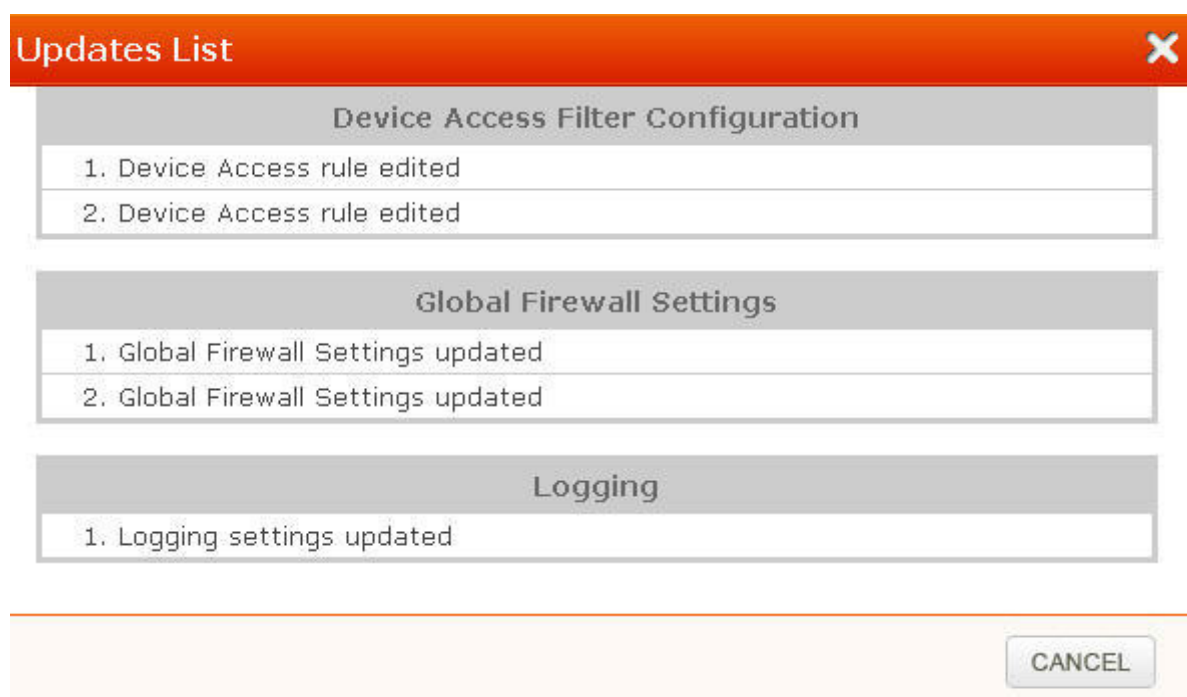


Figura 9: Configuración de Dispositivo

El número de cambios de configuración aparecerá sobre la izquierda del botón 'Apply Changes'. Para visualizar los detalles de los cambios de configuración, el usuario puede hacer clic en el ícono del número, el cual abrirá la lista de los cambios de configuración.

El usuario puede aplicar los cambios de configuración al dispositivo, haciendo clic en el botón 'Apply Changes'. Al hacer clic en el botón 'Apply Changes', los cambios de configuración serán aplicados al sistema y la configuración actualizada se mantendrá permanentemente en el dispositivo.

En el caso de que un usuario quiera abandonar los cambios de configuración realizados, puede hacer clic en el botón Ignore Changes (Ignorar Cambios). Al hacer clic en el botón 'Ignore Changes', los cambios de configuración almacenados en la ubicación de almacenamiento temporaria serán descartados.



Para aplicar los cambios de configuración, se mostrará el botón 'Ignore Changes' y el usuario no puede elegir ignorar los cambios de configuración. El botón 'Ignore Changes' será deshabilitado solo cuando aún haya cambios de configuración pendientes que necesiten ser aplicados al dispositivo.



Si el administrador intenta configurar un elemento de configuración en el valor apropiado, el ícono de información sobre herramientas que aparece al lado de cada elemento de configuración suministrará los detalles del error.

Al hacer clic en el ícono de ayuda que aparece al lado del título de configuración, se abrirá la sección de ayuda que corresponde a la página de configuración actual.

3.1. Configuraciones Generales

La página de configuraciones generales permitirá configurar las configuraciones de host/red del SIP Firewall. El dispositivo que ha sido creado para funcionar en modo puente, pero puede ser elegido para trabajar con asignación de IP estática o para adquirir la IP del dispositivo a través de DHCP.

La página además permite habilitar/deshabilitar el Acceso SSH al dispositivo. La opción 'Allow ICMP' (Permitir ICMP) configurará el dispositivo para responder o no a los mensajes ICMP enviados al SIP Firewall.

Por el Acceso SSH y el ICMP, los mensajes Ping para el SIP Firewall son permitidos.

General Settings

Device Settings

Host Name: sip_secure

IP Configuration: DHCP

IP Addr/Mask:

Gateway:

Dns Server:

Enable SSH: ☒

SSH Port: 22

Allow ICMP: ☒

Mgmt Vlan Addr/Mask: 192.168.100.1 / 255.255.255.0

Save Cancel

Figura 10: Configuraciones Generales

3.2. Configuraciones de Hora

El administrador puede elegir establecer las configuraciones de hora en el dispositivo o configurar el dispositivo para sincronizar las configuraciones de hora desde un servidor NTP. Se deben establecer las configuraciones/zonas horarias apropiadas en el dispositivo para que los cambios recientes aparezcan en las alertas de seguridad SIP generadas por el dispositivo.

Date / Time Settings

Date / Time Settings

Configuration Type: NTP

Date/Time: 10 : 15 : 01 / 09 / 2014

Time Zone: Africa/Abidjan

NTP Server:

Add Delete

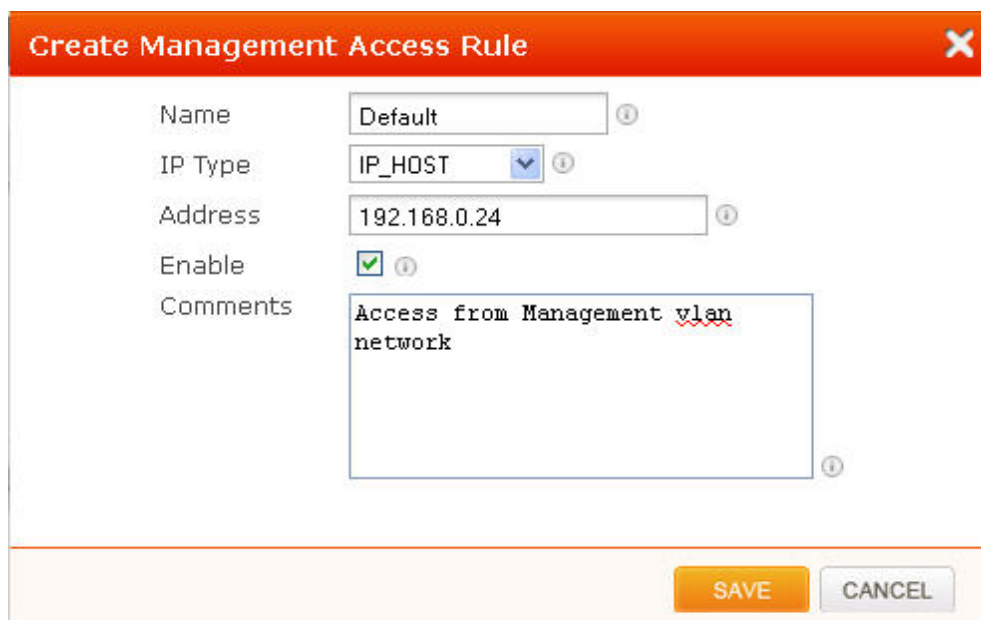
3.in.pool.ntp.org
4.in.pool.ntp.org

Apply Cancel

Figura 11: Configuraciones de Fecha/Hora

3.3. Gestión de Acceso

El acceso a la gestión del SIP Firewall (Acceso SSH CLI / WebUI) puede ser restringido con filtros de gestión de acceso. Por defecto, el acceso ha sido habilitado para cualquier dirección global y gestión de configuraciones de red VLAN del dispositivo. El administrador puede anular esta configuración.



Create Management Access Rule

Name: Default

IP Type: IP_HOST

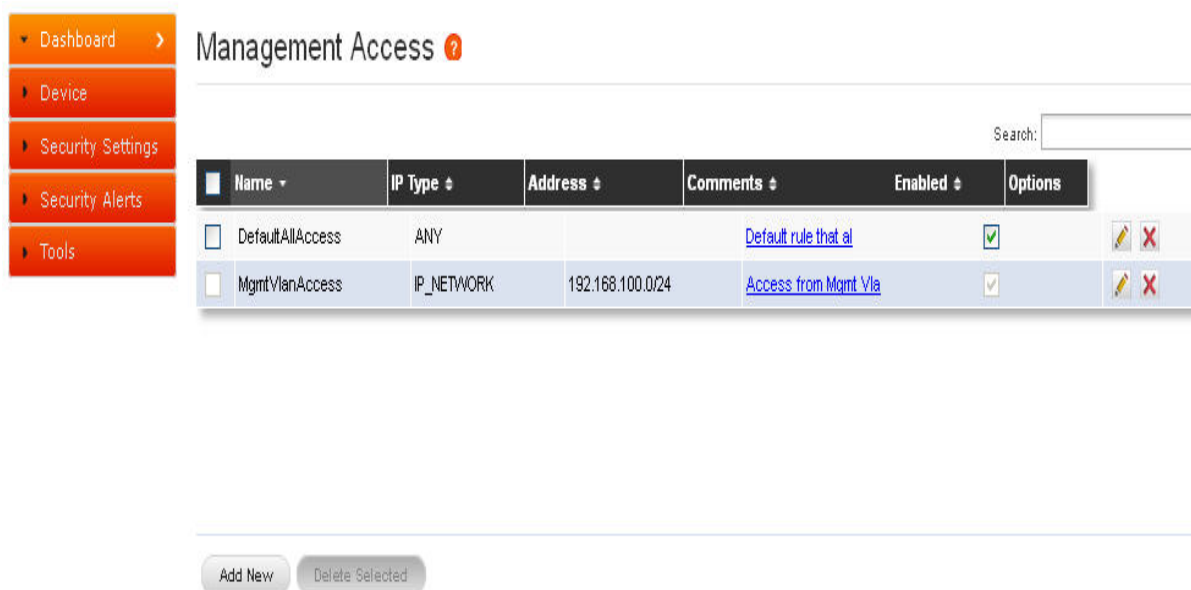
Address: 192.168.0.24

Enable: ☒

Comments: Access from Management vlan network

SAVE CANCEL

Figura 12: Norma para Crear Gestión de Acceso



Dashboard > Management Access ?

Search:

Name	IP Type	Address	Comments	Enabled	Options
☐ DefaultAllAccess	ANY		Default rule that al	☒	
☐ MgmtVlanAccess	IP_NETWORK	192.168.100.0/24	Access from Mgmt Vlan	☒	

Add New Delete Selected

Figura 13: Gestión de Acceso

El administrador necesita configurar la Dirección IP o la Red IP o el Rango de las Direcciones IP que tendrán acceso al equipo y debe(n) ser habilitada(s) en las reglas de filtro de gestión de acceso. El Tipo de IP 'ANY' (Cualquiera) indica redes globales (Cualquier red/Dirección IP).

La opción de búsqueda en los filtros de gestión de acceso ayudará a visualizar selectivamente las normas de filtro de gestión de acceso cuyos valores de nombre/dirección coincidan con el criterio de búsqueda.

3.4. Actualización de Firma

Para habilitar la actualización de firma automática, seleccione la casilla 'enable update' (habilitar actualización) en el dispositivo y configure la programación de actualización de firma. La clave de suscripción válida y la URL de actualización de la firma correcta deben ser configuradas para que ocurra la actualización de firma.

Para actualizar las firmas en el dispositivo de forma instantánea, haga Clic en el botón 'Update Signatures now' (Actualizar Firmas ahora).

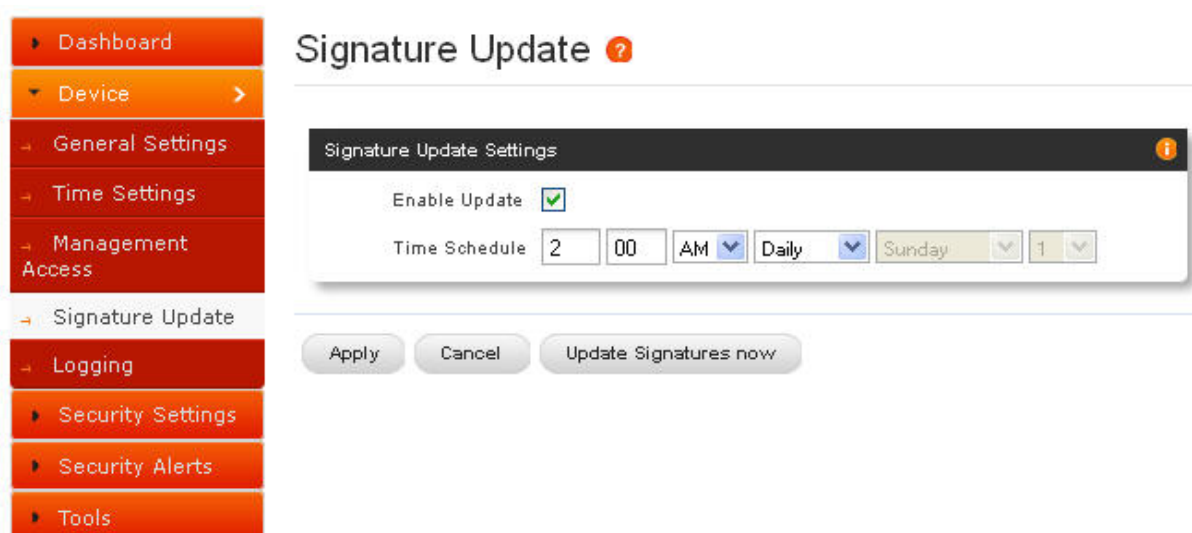


Figura 14: Actualización de Firma



Cuando el usuario compra un Elastix Firewall SIP, el dispositivo será enviado con las firmas SIP que ayudarán a protegerlo contra los ataques conocidos hasta el momento basados en SIP.

Sin embargo, si el usuario quiere asegurarse de que las implementaciones tengan la protección contra los vectores de ataque más nuevos, se recomienda habilitar la actualización de firma en el dispositivo.

Por favor, consulte con un representante de Ventas de Elastix para obtener los detalles de compra de la suscripción de firmas del SIP Firewall.

3.5. Registro

El administrador puede configurar el SIP Firewall para enviar las alertas de seguridad generadas al detectar ataques basados en SIP, al servidor SYSLOG remoto.

La página de registro permitirá habilitar/deshabilitar el registro remoto de las alertas de seguridad y hacia que servidor SYSLOG se debe redirigir las alertas de seguridad.

The screenshot displays the Elastix web interface. On the left, a vertical sidebar menu lists various system settings: Dashboard, Device, General Settings, Time Settings, Management Access, Signature Update, Logging (highlighted with a right-pointing arrow), Security Settings, Security Alerts, and Tools. The main area on the right is titled 'Logging' and contains a configuration modal. This modal has a dark header with the word 'Logging' and an information icon. Inside the modal, the 'Remote Logging' option is enabled, indicated by a green checkmark icon. Below it, the 'Syslog server' field contains the IP address '192.168.0.109', followed by an information icon. At the bottom of the modal, there are two buttons: 'Save' and 'Cancel'.

Figura 15: Registro

4. Configuración de las Políticas de Seguridad SIP

4.1. Políticas de Detección de Ataques SIP

La página de detección de Ataque SIP permite configurar las categorías de normas de Inspección Profunda de Paquete SIP. El administrador puede habilitar/deshabilitar la inspección contra una categoría de norma en particular, acción a ser tomada para detectar ataques coincidentes con las normas en las categorías.

Las acciones posibles que el SIP Firewall puede ejecutar son el registro de alerta, el bloqueo de los paquetes que contienen un vector de ataque y enviar a la lista negra la IP del atacante por un tiempo determinado. La duración del bloqueo en referencia a la cantidad de tiempo que un atacante necesita ser bloqueado también está configurada por nivel de categoría.

Category	Action	Blocking Duration (seconds)	Enabled	Options
Reconnaissance Attacks	Log	none	☐	
Sip Devices Scanning	Block	120	☒	
SIP Extensions Discovery	Block	120	☒	
Multiple Authentication Failures/Bruteforce password cracking Attempt	Block	1800	☒	
Ghost calls Attempt	Block	1800	☒	
SIP Protocol Compliance	Log	none	☒	
Sip Anomaly Attacks	Block	1800	☒	
Sip Dos Attacks	Block	1800	☒	
Sip DDos Attacks	Block	1800	☒	
Sip Cross site scripting Attacks	Block	1800	☒	

Figura 16: Detección de Ataque SIP

La tabla siguiente detalla las categorías de normas de Inspección Profunda de Paquete SIP soportadas en el SIP Firewall, y los parámetros de configuración en cada categoría.

Categoría	Descripción	Opciones Configurables de Usuario
Ataques de Reconocimiento SIP	El intruso está tratando de detectar qué versión de Asterisk usted está ejecutando. Con esa información, él comenzará a aprovecharse de las numerosas vulnerabilidades de esa versión. El Firewall SIP no responderá a esta solicitud.	N/A
Escaneo de Dispositivos SIP	El intruso escaneará los puertos PBX para ver qué dispositivos están conectados a él. Con esa información, él puede aprovecharse de las vulnerabilidades de 3ros. El SIP Firewall no responderá a su solicitud.	N/A
Descubrimiento de Extensiones SIP	El intruso le pedirá al PBX que divulgue el rango de los números de extensión. Con esa información, él puede probar diferentes claves para tomar control de estas extensiones. El SIP Firewall no responderá a esa solicitud.	Intentos/Duración de Registro de Usuario SIP Inválido
Múltiples Intentos Fallidos/Fuerza Bruta de Autenticación de Clave	El intruso intentará iniciar sesión con diferentes nombre de usuario y claves muchas veces. Una vez que tenga éxito, tendrá control de esa extensión. El SIP Firewall puede bloquear, registrar o colocar en la lista negra la IP por un período de tiempo si excede el número de intentos/segundos autorizados.	Intentos/Duración de Autenticación Fallidos
Intento de Llamadas Fantasma	El intruso generará llamadas a una extensión y parecerá como si provinieran de la misma extensión. Su objetivo es quebrar el PBX y lograr interrumpir la comunicación. El SIP Firewall puede bloquear, registrar o colocar en la lista negra la IP por un período de tiempo si excede el número de intentos/segundos autorizados.	Sin Respuesta/Duración de Invitación de Anónimos
Ataques de SIP Dos	Intentos de desbordamiento usando varios mensajes SIP.	Sin Mensajes/Duración de

		Solicitud de SIP
Ataques SIP DDos	Intentos de desbordamiento distribuidos usando varios mensajes SIP.	Sin Mensajes/Duración de Respuesta SIP
Ataques de Anomalía SIP	El intruso enviará paquetes de SIP anormales al PBX. Su objetivo es quebrar el PBX logrando interrumpir la comunicación. El SIP Firewall puede bloquear, registrar o colocar en la lista negra la IP por un período de tiempo si excede el número de intentos/segundos autorizados.	N/A
Ataques Desbordamiento del Buffer del SIP	Los intentos de desbordamiento de Buffer resultaron de validación impropia de ingresos de usuario.	N/A
Escritura de sitios Cruzados de SIP	SIP es vulnerable a cross-site scripting, causado por validación impropia de ingresos suministrados por el usuario en la solicitud SIP. Un atacante remoto podría aprovecharse de esta vulnerabilidad para inyectar escritura maliciosa dentro de una página web, la cual será ejecutada en el navegador Web de la víctima, cuando la víctima acceda a una página web que contiene información tomada de la solicitud SIP.	N/A
Vulnerabilidades de garantías de 3ros.	Ataques con objetivos hacia equipos y/o gateways PBX/SIP aprovechándose de su vulnerabilidad.	N/A

4.2. Protocolo de Cumplimiento SIP

El *motor de Inspección Profunda de Paquete SIP* que corre en el SIP Firewall ha sido creado para inspeccionar el tráfico SIP con las normas de Cumplimiento de Seguridad SIP para integrarlo con el motor SIP DPI.

Las anomalías en los encabezados de Mensaje SIP pueden resultar por varias condiciones erróneas, fallas de analizador SIP y paquetes malformados, los cuales llevarán a las aplicaciones SIP a ser vulnerables para el ataque.

Los siguientes parámetros serán usados por el motor de paquete profundo SIP para identificar las condiciones de anomalía de protocolo diferentes y tomar medidas configuradas por el administrador.



Configurando los valores inapropiados para estos parámetros puede resultar en el impacto disruptivo en la implementación VOIP. Los administradores con mayor conocimiento del protocolo SIP pueden elegir calibrar estos parámetros para sus necesidades de implementación específica. De lo contrario, se recomienda usar los marcos por defecto de estos parámetros.

Figura 17: Cumplimiento de Protocolo SIP

Max_sessions

Una sesión SIP es la conexión creada, a nivel de aplicación, entre el servidor SIP y el cliente SIP para intercambiar mensajes de audio/video.

El parámetro max_sessions define la sesión de número máximo que el *motor de inspección profunda de paquete* SIP puede controlar. El valor por defecto ha sido establecido en 4096.

Max Diálogos por sesión

Max_Dialogs_per_session especifica el número máximo de transacción de mensajes SIP que pueden darse entre el servidor y el cliente SIP.

Métodos

Esto especifica qué métodos revisar para los mensajes SIP. Los siguientes son los mensajes SIP que el motor SIP DPI puede identificar: (1) invite, (2) cancel, (3) ack, (4) bye, (5) register, (6) options, (7) refer, (8) subscribe, (9) update, (10) join, (11) info, (12) message, (13) notify, (14) prack.

Max_uri_len

El Uri (identificador de recursos uniformes) identifica el usuario o servicio hacia el cual la solicitud SIP está siendo dirigida. Max_uri_len especifica el tamaño máximo del campo de Solicitud URI. El predeterminado está establecido en 256. El rango permitido para esta opción es 1 - 65535.

Max_call_id_len

El campo Call-ID del encabezado en el mensaje SIP actúa como un identificador único que se relaciona con la secuencia de mensajes intercambiados entre el cliente SIP y el servidor. Max_call_id_len especifica tamaño de campo máximo de Call-ID. El predeterminado está establecido en 256. El rango permitido para esta opción es 1 - 65535.

Max_requestName_len

Max_requestName_len especifica el tamaño máximo de solicitud de nombre (*request name*) que es parte de la ID CSeq. El predeterminado está establecido en 20. El rango permitido para esta opción es 1 – 65535.

Max_from_len

El campo del encabezado *From* indica la identidad del iniciador de la solicitud SIP. Max_from_len especifica el máximo tamaño del campo *from*. El rango permitido para esta opción es 1 - 65535.

Max_to_len

El campo del encabezado *to* especifica el receptor deseado de la solicitud SIP. Max_to_len especifica el máximo para el tamaño del campo *to*. El predeterminado está establecido en 256. El rango permitido para esta opción es 1 - 65535.

Max_via_len

El campo del encabezado *Via* indica el medio usado para la transacción SIP e identifica la ubicación donde la respuesta SIP debe ser enviada.

Max_via_len especifica el máximo tamaño del campo *Via*. El predeterminado está establecido en 1024. El rango permitido para esta opción es 1 - 65535.

Max_contact_len

El identificador usado para contactar una instancia específica del cliente/servidor SIP para solicitudes subsecuentes. Max_contact_len especifica el máximo de tamaño del

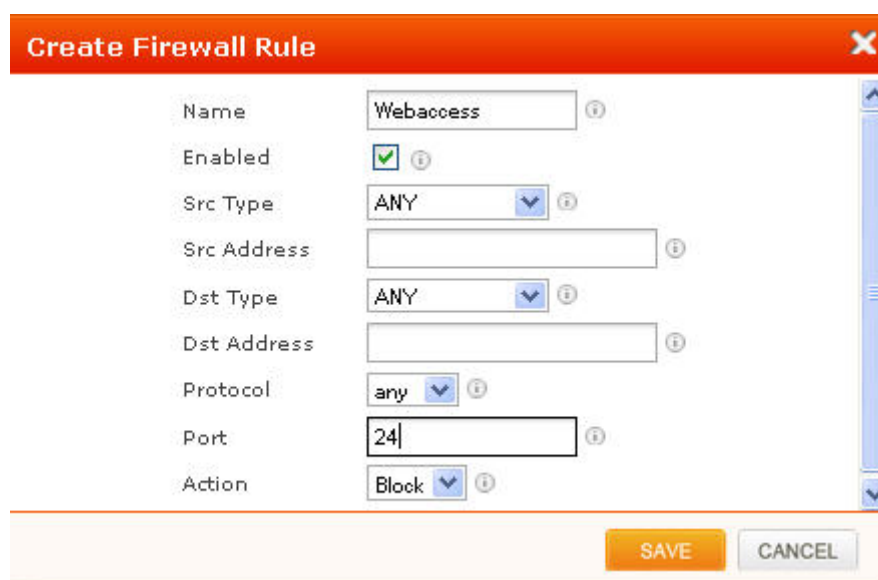
campo Contact. El predeterminado está establecido en 256. El rango permitido para esta opción es 1 - 65535.

Max_content_len

Especifica el tamaño máximo del contenido del cuerpo del mensaje. El predeterminado está establecido en 1024. El rango permitido para esta opción es 1 - 65535.

4.3. Normas Firewall

La configuración de las normas de firewall permitirán al administrador configurar qué tráfico debe ser permitido para proteger la red SIP PBX/Gateway de una zona wan no confiable, además del tráfico DPI permitido SIP y RTP. El administrador necesita especificar las redes fuente y de destino y los números de puerto y protocolo que serán usados como criterios coincidentes en las normas de filtro y las acciones a ser tomadas en normas de filtro coincidentes. Las acciones posibles bloquearán el tráfico y permitirán el tráfico de normas de filtrado coincidente. El precedente de las normas estará en el orden en el cual las normas se configuraron en la tabla de normas de firewall.



The screenshot shows a 'Create Firewall Rule' window. The fields are as follows:

Field	Value
Name	Webaccess
Enabled	☒
Src Type	ANY
Src Address	
Dst Type	ANY
Dst Address	
Protocol	any
Port	24
Action	Block

Figura 18: Crear Norma Firewall

4.4. Configuración de Firewall

Las Configuraciones de Firewall permiten al usuario configurar *TCP Flood Rate*, *TCP Flood Burst*, *UDP Flood rate* y *UDP Flood Burst* en configuraciones firewall globales.

Figura 19: Configuraciones Firewall

4.5. Normas de Lista Blanca

Esta página permite configurar las direcciones IP en la lista blanca dentro de la zona wan no confiable desde donde el acceso para comunicarse con la red SIP protegida será permitida por la SIP Firewall.

Esta página también permitirá configurar si las normas blancas toman precedencia sobre las normas de la lista negra (tanto estáticas como dinámicas) configuradas en el dispositivo en cualquier instante.

Figure 20: Crear Norma de lista Blanca

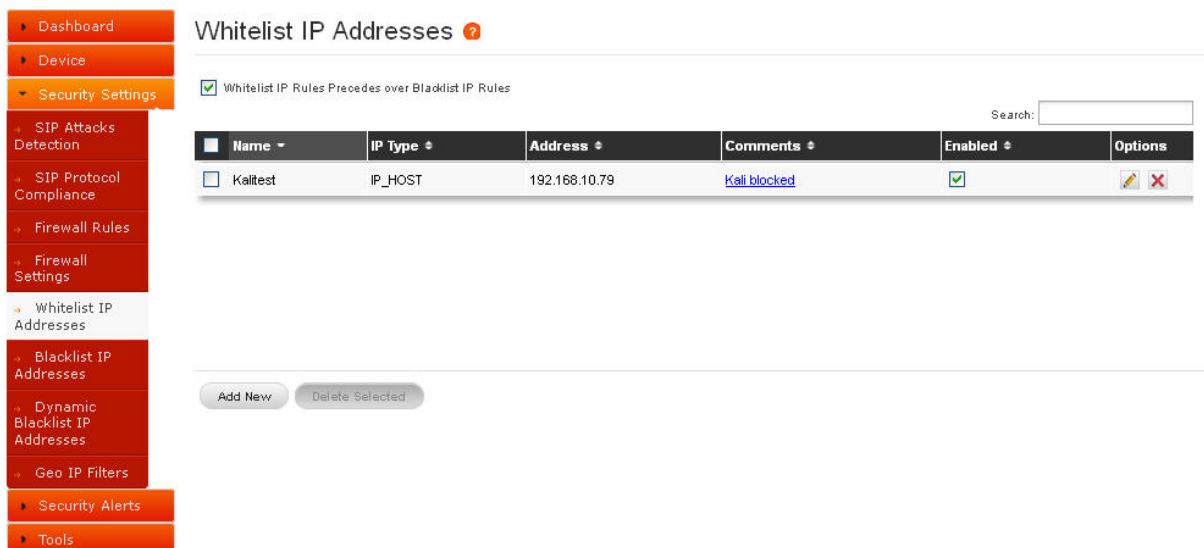


Figura 21: Direcciones IP de Lista Blanca

4.6. Normas de Lista Negra (Estática)

Esta página permite configurar las direcciones IP de la lista negra en la zona wan no confiable desde donde el acceso para comunicarse con la red SIP protegida será bloqueada por el SIP firewall.

Esta página también permitirá configurar si las normas blancas toman precedencia sobre las normas de la lista negra (tanto estática como dinámica) configuradas en el dispositivo en cualquier instante.

Create Blacklist Rule

Name: Kallitest

IP Type: IP_HOST

Address: 192.168.10.79

Enable: ☒

Comments: Kali blocked

SAVE CANCEL

Figura 22: Crear Norma de Lista Negra

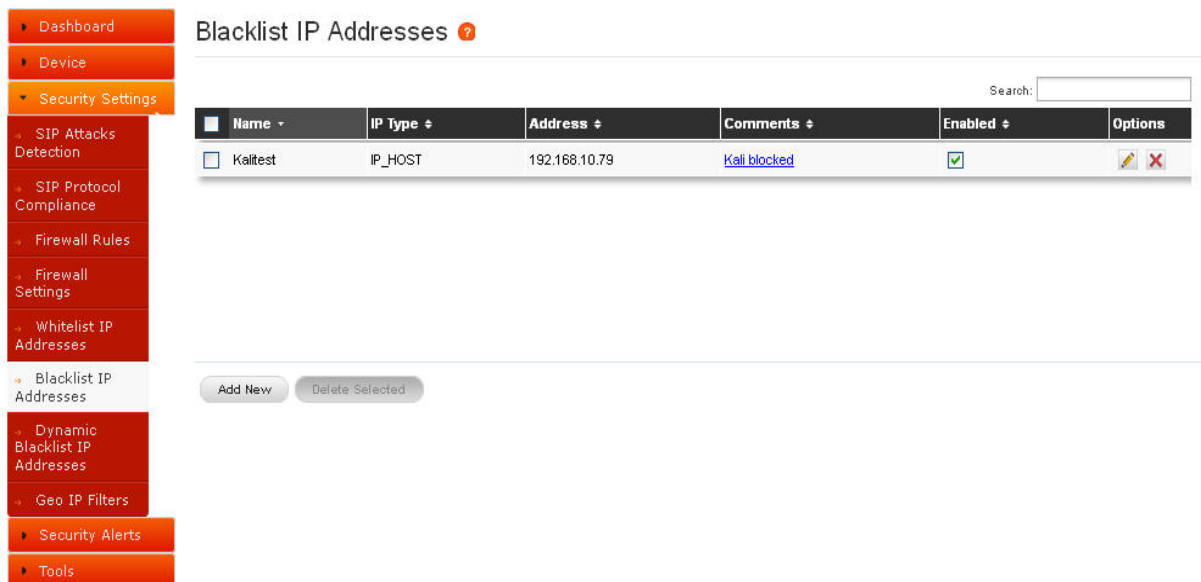


Figura 23: Direcciones IP de Lista Negra

4.7. Normas de Lista Negra Dinámica

Las normas de la lista negra dinámica son las normas de bloqueo agregadas por el *motor de inspección profunda de paquetes* del SIP Firewall para bloquear el tráfico de direcciones IP de atacantes por la duración de bloqueo configurada en la categoría de normas para detectar el ataque.

Las normas de lista negra dinámica permitirán al administrador ver las normas de lista negra dinámicas configuradas actualmente en el dispositivo en cualquier momento. En caso de que el administrador quiera ignorar y permitir el tráfico de una dirección IP de lista negra en particular, él puede eliminar la norma de la página de normas de lista negra dinámica.



Figura 24: Direcciones IP de Lista Negra Dinámica

4.8. Filtro IP Geo

El administrador puede elegir bloquear el tráfico proveniente de países específicos hacia la red SIP protegida, configurando las normas de filtro GeoIP en el SIP Firewall.

The screenshot displays the 'Geo IP Filters' configuration page. On the left is a sidebar with navigation links: Dashboard, Device, Security Settings (expanded), SIP Attacks Detection, SIP Protocol Compliance, Firewall Rules, Firewall Settings, Whitelist IP Addresses, Blacklist IP Addresses, Dynamic Blacklist IP Addresses, Geo IP Filters (selected), Security Alerts, and Tools. The main content area has a title 'Geo IP Filters' with a help icon. Below the title are three buttons: 'Allow All Countries', 'Block All Countries', and 'Update Geo IP'. A search bar is located on the right. The main part of the page is a table with three columns: 'Country Name', 'Allowed', and 'Options'. The table lists several countries, all of which are currently 'Allowed' (indicated by a green checkmark). Each row has an 'Options' column with an edit icon (pencil) and a delete icon (trash). The countries listed are: RUSSIAN FEDERATION, SYRIAN ARAB REPUBLIC, SUDAN, NIGERIA, KOREA, REPUBLIC OF, CHINA, UKRAINE, and ALGERIA.

Country Name	Allowed	Options
RUSSIAN FEDERATION	☒	 
SYRIAN ARAB REPUBLIC	☒	 
SUDAN	☒	 
NIGERIA	☒	 
KOREA, REPUBLIC OF	☒	 
CHINA	☒	 
UKRAINE	☒	 
ALGERIA	☒	 

Figura 25: Filtros de IP Geo

5. Estado

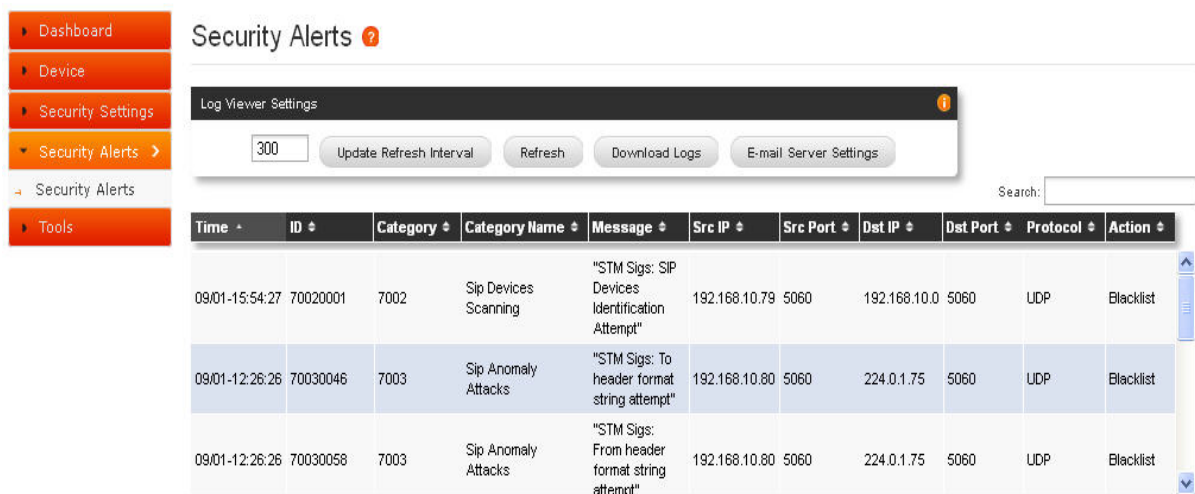
5.1. Alertas de Seguridad

La página de alertas de estado muestra la lista de alertas pertenecientes a los ataques SIP detectados en el *motor de inspección profunda de paquete* del SIP Firewall en cualquier instante.

El administrador puede elegir establecer el intervalo de carga en el visualizador de logs en esta página.

El administrador puede elegir configurar el dispositivo para enviar resúmenes de notificaciones por email sobre las alertas de seguridad generadas por el dispositivo.

La opción para descargar las alertas de seguridad mostrada en esta página en formato CSV está disponible en la página.



Time	ID	Category	Category Name	Message	Src IP	Src Port	Dst IP	Dst Port	Protocol	Action
09/01-15:54:27	70020001	7002	Sip Devices Scanning	"STM Sigs: SIP Devices Identification Attempt"	192.168.10.79	5060	192.168.10.0	5060	UDP	Blacklist
09/01-12:26:26	70030046	7003	Sip Anomaly Attacks	"STM Sigs: To header format string attempt"	192.168.10.80	5060	224.0.1.75	5060	UDP	Blacklist
09/01-12:26:26	70030058	7003	Sip Anomaly Attacks	"STM Sigs: From header format string attempt"	192.168.10.80	5060	224.0.1.75	5060	UDP	Blacklist

Figura 26: Alertas de Seguridad



A menos que el usuario configure el reenvío de alertas de seguridad al servidor remoto SYSLOG, las alertas de seguridad no continuarán permanentemente en el dispositivo. La ubicación del buffer de registro será descartada en el intervalo predeterminado (no configurable) una vez que los criterios de entrada de registro sean alcanzados. Sin embargo, si el administrador quiere continuar las alertas dentro del almacenamiento USB, puede conectar el almacenamiento USB al puerto de datos USB del Elastix SIP Firewall.

6. Herramientas

6.1. Administración

La página de interfaz del usuario brinda la opción de ejecutar un reinicio de fábrica en el dispositivo, reiniciando el dispositivo, *device reboot* (reinicio de dispositivo), *device shutdown* (apagar dispositivo) y *Configuration backup/restore* (copia de respaldo/reestablecer configuración).

Ejecutar el reinicio de fábrica en el dispositivo requiere reiniciar, por consiguiente, el administrador será redirigido a la página de notificación de espera al hacer clic en el botón de reinicio de fábrica y se registrará rápidamente una vez que el dispositivo haya logrado la configuración por defecto.

Los SIP Firewall de Elastix soportan tomar la copia de respaldo de la configuración y reestablecer la configuración más tarde.

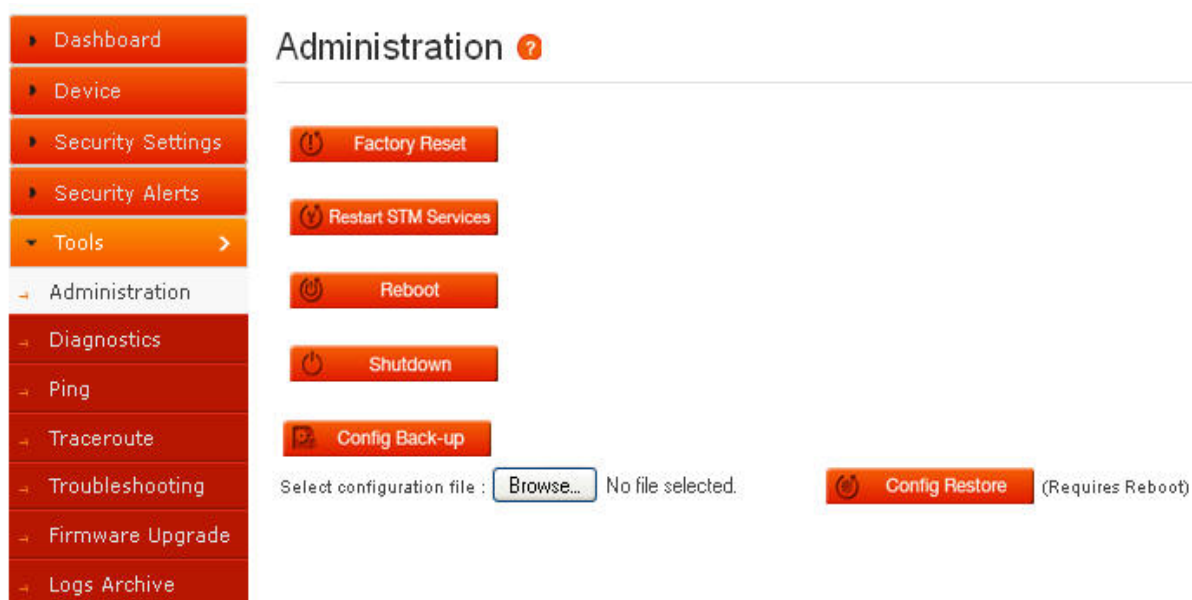


Figura 27: Administración



La copia de respaldo de la configuración contará con la configuración continuada últimamente, si hay algunos cambios transitorios que aún debieran ser aplicados mientras se realiza la copia de seguridad; esos cambios de configuración no serán incluidos en el archivo de la copia de respaldo de la configuración.

6.2. Diagnósticos

La página de diagnósticos permitirá al administrador recoger los registros problemáticos que ayudarán al equipo de soporte de Elastix a depurar cualquier tema enfrentado a la implementación de instalación del SIP Firewall.

Para ejecutar la utilidad en el dispositivo, el administrador necesita hacer clic en el botón 'Run Diagnostics' (Ejecutar Diagnósticos). El dispositivo ejecutará la tarea de diagnóstico en segundo plano y mostrará los resultados una vez que se haya completado. El administrador puede descargar los reportes haciendo clic en el botón 'Get Report' (Obtener Informe) y enviar el informe al equipo de soporte de Elastix (**Nota:** Usted puede enviar un email a support@elastix.com)

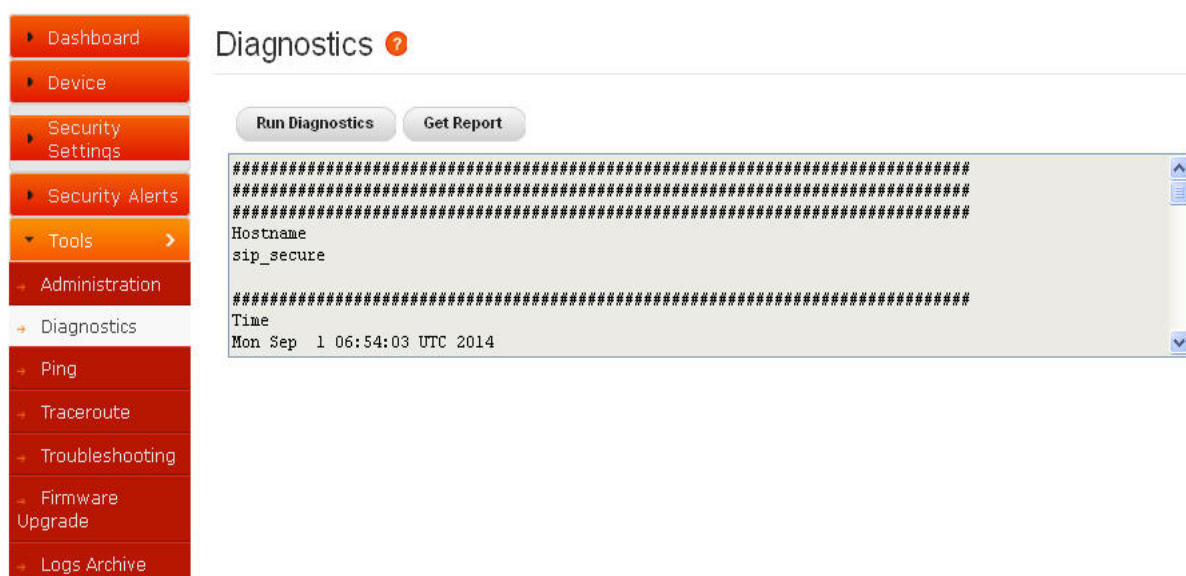


Figura 28: Diagnósticos

Haga clic en el enlace de abajo para descargar los diagnósticos.



Figura 29: Descargar Informe

6.3. Ping

El administrador puede resolver los temas de conectividad de la red con la ejecución ping desde el dispositivo SIP Firewall.

El administrador necesita ingresar la dirección IP que necesita ser comprobada desde el SIP Firewall, seleccionar el conteo de ping (*Count*) y hacer clic en el botón 'Ping' para ejecutar la tarea. Los resultados del ping serán mostrados en el área de texto una vez que la tarea ping se haya completado.



Figura 30: Resultado Ping

6.4. Trace Route

El administrador puede resolver los temas de conectividad de la red ejecutando un trace route desde el dispositivo SIP Firewall.

El administrador necesita ingresar la dirección IP hacia la cual se debe trazar la ruta desde el SIP Firewall, seleccionar el conteo de hop y hacer clic en el botón '*Trace route*' (Seguir ruta) para ejecutar la tarea.

Los resultados de la ruta de seguimiento serán mostrados en el área de texto una vez que la tarea de ruta de seguimiento haya sido completada.

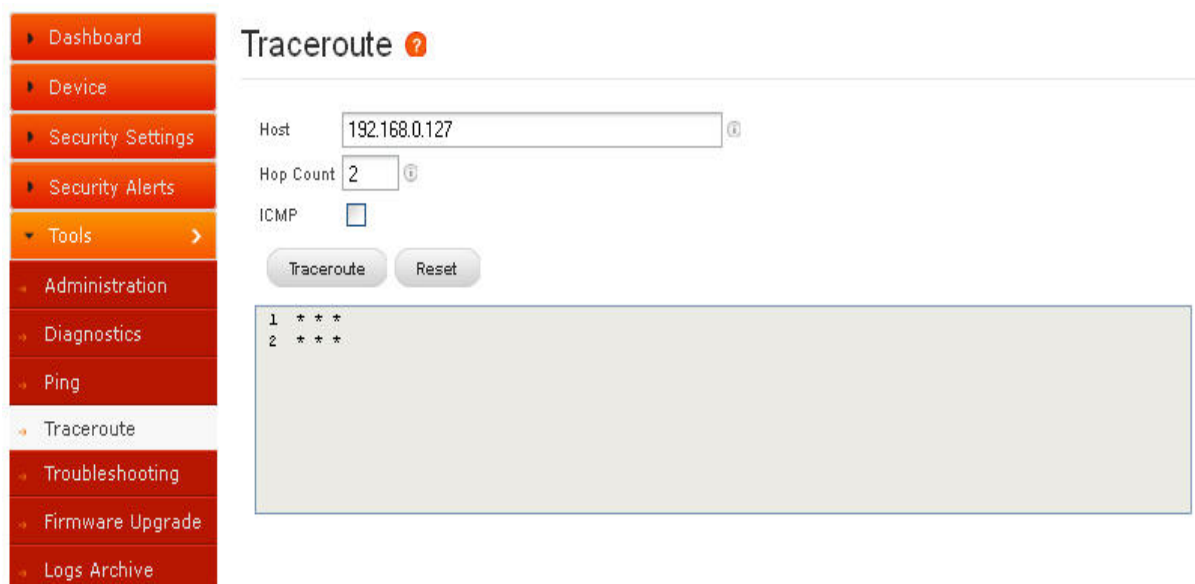


Figura 31: Ruta de Seguimiento

6.5. Solución de Problemas

Esta página permitirá deshabilitar/habilitar el DPI en el SIP Firewall para propósitos de solución de problemas.

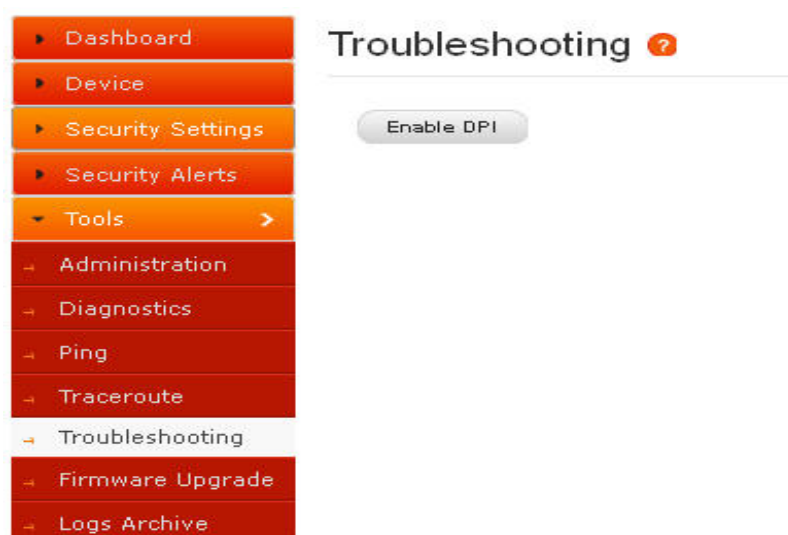


Figure 32: Solución de Problemas

6.6. Actualización de Firmware

El SIP Firewall soporta la actualización manual del firmware que se ejecuta en el equipo. La página de actualización de firmware muestra la versión del firmware del SIP Firewall actualmente en ejecución y permite al administrador cargar el paquete de actualización del firmware e instalarlo en el dispositivo.

Para instalar el firmware,

- Descargar el paquete de actualización de firmware del SIP Firewall desde la página web de Elastix y guardarlo en su sistema local.
- Desde el navegador de su sistema local, inicie sesión en WebUI del SIP Firewall y abra la página de actualización de firmware de SIP Firewall.
- Haga clic en 'Browse' (Explorar) en la página del firmware y seleccione el archivo del paquete de actualización del firmware del SIP Firewall que usted guardó en su sistema local
- Luego de seleccionar el archivo, haga clic en el botón 'Upgrade' (Actualizar).
- El dispositivo verificará que el firmware se cargue y se instale. Luego de instalarlo, el dispositivo se reiniciará y el administrador será redirigido a la página de inicio de sesión.

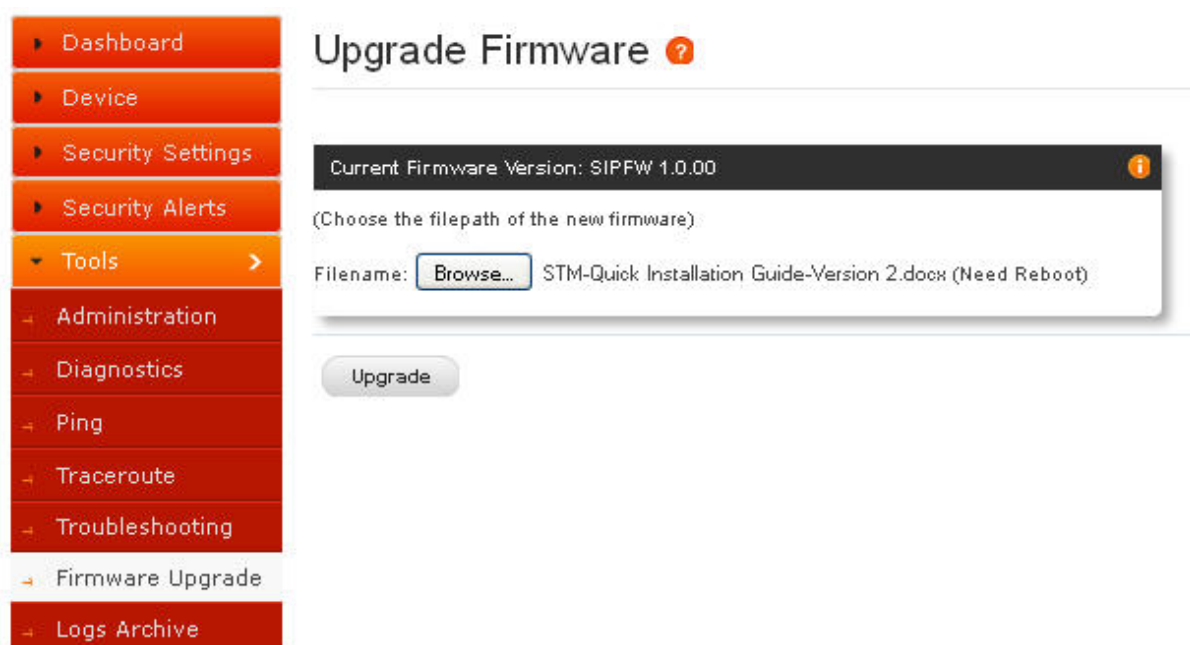


Figura 33: Actualizar Firmware

6.7. Archivo de Registros

Si el dispositivo de almacenamiento USB se adjuntó al SIP Firewall, el dispositivo intentará archivar los registros más antiguos en el dispositivo de almacenamiento USB. La información de resumen en los registros almacenados en el archivo será mostrada en la Página de Archivos de Registros.



Figura 34: Archivos de Registros

La página de Administración de interfaz de usuario brinda la opción de ejecutar un reinicio de fábrica en el dispositivo, *restarting the device*, *device reboot*, *device shutdown* y *Configuration backup/restore*.

Ejecutar el reinicio de fábrica en el dispositivo requiere reiniciar el dispositivo, por consiguiente, el administrador será redirigido a la página de notificación de espera al hacer clic en el botón de reinicio de fábrica y se le solicitará rápidamente iniciar sesión una vez que el dispositivo aparezca con la configuración por defecto.

Los SIP Firewall soportan tomar la copia de respaldo de configuración y almacenar la configuración más tarde.

APÉNDICE

7. Apéndice A – Usando Acceso de Consola

1. Conecte la consola de serie al puerto serie del dispositivo SIP Firewall.
2. Use las siguientes configuraciones de consola serie para acceder a 'Elastix' CLI
 - i. Velocidad: 38400
 - ii. Paridad : Ninguna
 - iii. Fecha : 8
 - iv. Bits de Detención: 1
 - v. Control de Flujo : No
3. El usuario debe ver el comando 'Elastix' rápidamente en la terminal
4. Escriba 'help' (ayuda) para visualizar la lista de comandos de solución de problemas disponibles.

8. Apéndice B – Configuración de la Dirección IP del SIP Firewall a través de la Consola

El usuario puede elegir visualizar/establecer la dirección IP del dispositivo SIP Firewall Elastix > show IP

Ahora usted puede acceder al dispositivo desde el navegador usando la URL <https://<device-ip>>



Si usted no está ejecutando el servidor DHCP en su implementación O el dispositivo falla al obtener la dirección IP, establezca la dirección IP desde la consola CLI usando la línea de comando.

Elastix > Set IP < IP address><mask><gateway>

Verifique la dirección usando el comando 'show IP' (mostrar IP). Luego, use esta dirección IP para acceder a la WebUI/SSH para configurar el dispositivo para realizar más configuraciones.



Ante cualquier asistencia técnica requerida, por favor, contáctese con el soporte al email

support@elastix.com